WPA

Plan

- I. Présentation
  - 1°) WPA
  - 2°) WPA2
- II. L'Association WiFi
  - 1°) Base
  - 2°) Avec un serveur d'authentification
  - 3°) Plus en détail
- III. Résumé

I. Présentation

- Définition :
  - Mécanisme de sécurité des réseaux sans-fil

- 1°) WPA
  - Fin 2002, Wi-Fi Alliance
  - TKIP

2°) WPA2

- Juin 2004, IEEE
- TKIP et AES

- Version personal : Clés partagées

- Version enterprise : Serveur d'authentification

II. L'Association WiFi

1°) Base (personal)

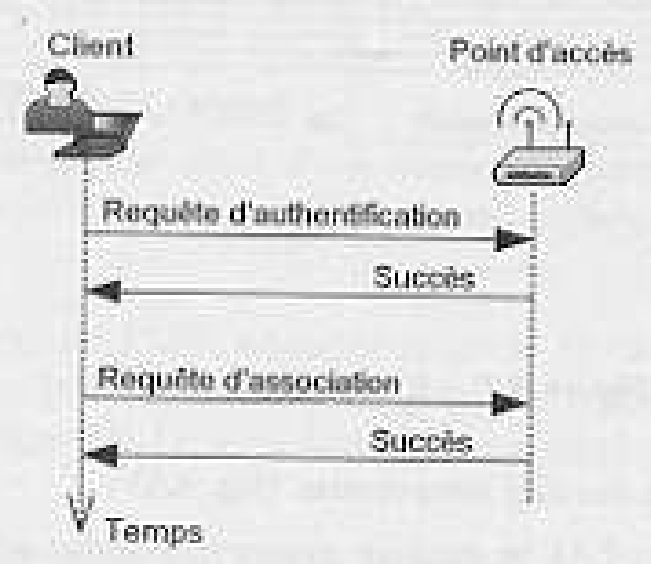

Fig1 : Association WiFi de base

2°) Avec un serveur d'authentification (enterprise)

- 802.1x

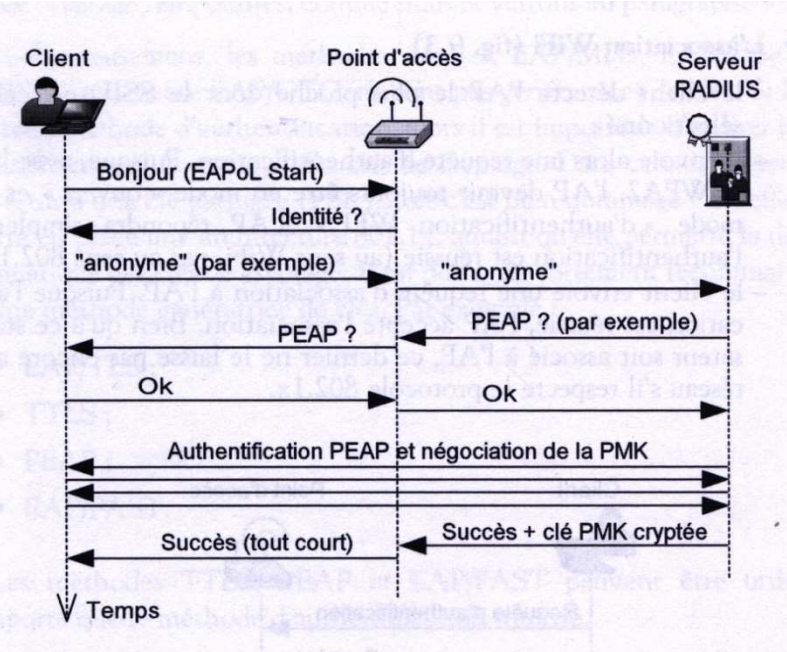

Fig2 : Association WiFi avec un serveur d'authentification

3) Plus en détail

- Les clés

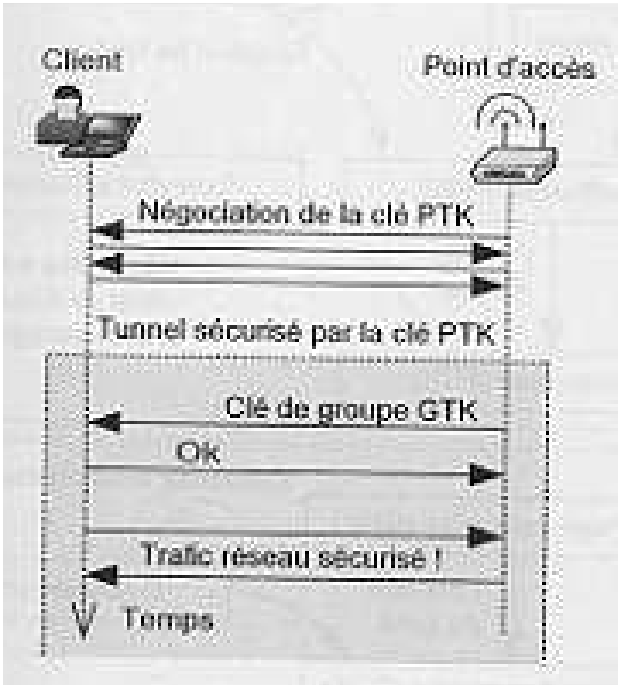

Fig3 : Négociation des clés

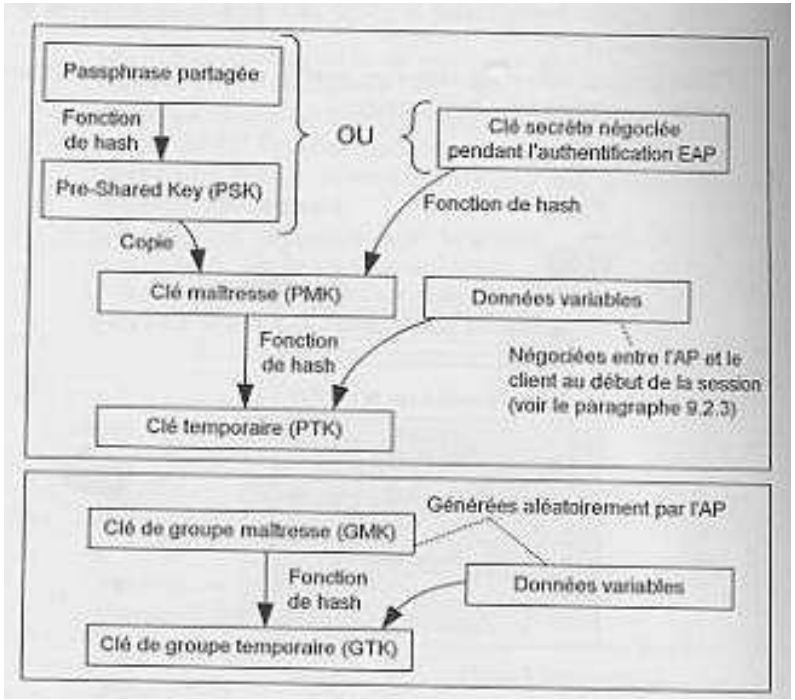

Fig4 : Hiérarchie des clés

3) Plus en détail

- Le four-way Handshake

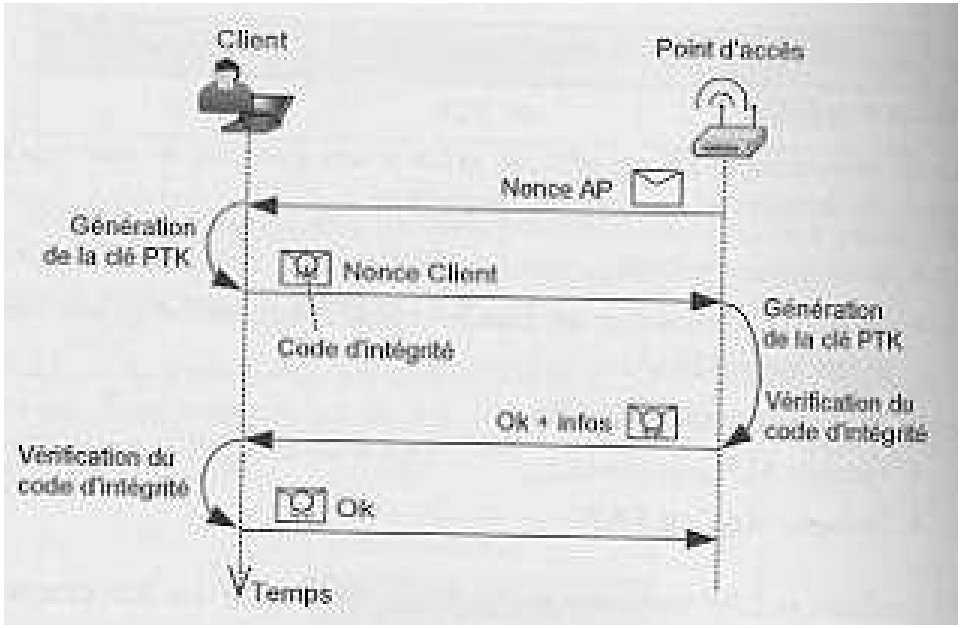

Fig5 : Le four-way Handshake

III. Résumé

Solution	Protocole	Cryptage	Intégrité
WEP	WEP	RC4	CRC
WPA	TKIP	RC4	Michael
WPA2	TKIP	RC4	Michael
WPA2	CCMP	AES	CBC

Conclusion :

- Mot de passe complexe
- Bonne sécurité du type WPA et WPA2

Merci de votre attention !

Si vous avez des questions ?